2.13 Ausencia de respaldos fuera de las instalaciones.

De la validación en terreno al datacenter del MIDESO, en el cual están alojados los servidores del SENADIS, se advirtió que los respaldos se mantienen en el mismo espacio físico, con lo que, en caso de algún siniestro, se afectaría la continuidad operativa de las labores efectuadas por la institución. Además, se detectó la ausencia de respaldos en otras dependencias, todo lo que no se condice con lo expresado en los literales d), e), g) del artículo 24, del antedicho decreto, sobre la gestión de las operaciones y las comunicaciones.

El servicio en su respuesta precisa, en síntesis, que se considerará en el proceso de elaboración de presupuesto 2018.

Considerando lo indicado en el párrafo precedente, se mantiene la observación formulada, por cuanto las acciones informadas no se han materializado, considerando que son posibles acciones a ejecutar con el presupuesto antes mencionado.

2.14 Inexistencia de trazabilidad de acciones efectuadas por usuarios de la base de datos y mecanismos de auditoría.

De la revisión ejecutada en la consola del servidor de base de datos Oracle, del sistema de remuneraciones, administrada por el Departamento de Informática, se constató que esta no posee restricciones de edición y/o eliminación de registros a nivel de usuarios, ni almacena el usuario que se conecta, en un LOG que identifique las acciones, como insertar, borrar, entre otras, lo que imposibilita realizar seguimientos a los cambios efectuados sobre ellas, lo que se aparta de lo estipulado en el artículo 23 del aludido decreto, de la gestión de las operaciones y las comunicaciones.

La repartición en su respuesta indica que el Encargado de la Sección de la Información realizará la restricción de perfiles a las bases de datos del servicio y habilitará la generación de LOG que den cuenta de la trazabilidad de las acciones efectuadas por los usuarios a las bases de datos.

Por lo anterior y habida consideración que las medidas indicadas no se han materializado, procede mantener la observación antes anotada en este punto, en tanto éstas no se implementen.

Las situaciones descritas en los puntos 2.1 al 2.14, conllevan los riesgos de falta de continuidad operacional, de inexistencia de registro de seguridad y de cambios, de pérdida de información, y la imposibilidad de efectuar trazabilidad a los datos y verificar su integridad, por lo que, además de incumplir los aspectos del decreto N° 83, de 2004, que en cada caso se indican, vulneran los principios de control, eficiencia y eficacia previstos en el artículo 3°, inciso segundo, de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

3. Falta de un procedimiento para filtrar SPAM[5].

Se acreditó la inexistencia de un procedimiento orientado a la filtración de correos electrónicos no deseados, situación también corroborada por el Jefe Sección Gestión de Información, mediante el referido correo electrónico de 28 de abril del año 2017.

La institución en su respuesta señala que elaborará un procedimiento de buen uso del correo electrónico, el cual abarcará entre otros aspectos, el manejo del SPAM.

En esas circunstancias, y en tanto no se compruebe por esta Contraloría General la implementación de las medidas correctivas anunciadas, se mantiene lo observado.

4. Inexistencia de un documento formalizado para gestionar la seguridad de la información.

Si bien se advirtió la existencia de del documento denominado "Procedimiento de Control y Registro de Incidentes de Seguridad", este no se encuentra formalizado, lo que no se condice con lo expresado en la letra a), del 37, del decreto N° 83, de 2004, sobre la existencia de una Política de Seguridad, ni en el artículo 3°, inciso segundo, de la ley N° 19.880, sobre Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado, que define al acto administrativo como la decisión formal que emite la administración y que contiene una declaración de voluntad, realizada en el ejercicio de una potestad pública, el que de acuerdo con el principio de escrituración, contemplado en el artículo 5° del mismo texto legal, se expresará por escrito.

El servicio señala que el Encargado de la Sección de la Información elaborará un procedimiento de gestión de incidentes, que permita gestionar y resolver incidentes de seguridad de la información con el fin de obtener trazabilidad de los procesos y reducir la posibilidad o el impacto de incidentes futuros.

Considerando lo indicado en el párrafo precedente, se mantiene la observación formulada, por cuanto las acciones informadas no se han materializado.

5 SPAM: Hace referencia a correo basura, son mensajes no solicitados, no deseados o con remitente no conocido, habitualmente de tipo publicitario, generalmente son envíos masivos.

III. EXAMEN DE CUENTAS

- Contratación de los servicios de Firma Electrónica Avanzada, sin utilización.

A través de la orden de compra ID N° 857-2978-CM14, de 29 de diciembre del año 2014, el SENADIS adquirió 25 token, 5 software de desarrollo y 25 certificados de firma electrónica avanzada Symantec e-GOVSIGN, por un monto ascendente a USD $ 31.824, equivalente a $ 19.353.796, IVA incluido, proyecto que posteriormente fue suspendido por el ya citado hackeo, y reiniciado en diciembre de 2015, con la habilitación de las precitados certificados, los cuales desde ese momento fueron válidos por un año.

Cabe señalar que el valor, por un año, de los referidos certificados fue de USD $ 4.180, que al tipo de cambio a igual fecha ascendió a $ 2.934.308, IVA incluido, los que expiraron en el mes de noviembre de 2016, sin que se haya demostrado que se hubiesen utilizado.

Sin embargo, mediante la orden de compra ID N° 857-1524-CM16, de 30 de septiembre del año 2016, se efectuó una nueva adquisición a la empresa e-SIGN, por la provisión de la "FIRMA ELECTRONICA AVANZADA E-SIGN SYMANTEC E-GOVSIGN 25 CERTIFICADOS" por un valor de $ 1.647.041, sin que a la fecha de cierre de la presente fiscalización, esto es, 6 de junio del año 2017, se presentaran evidencias que den cuenta de su uso.

La situación expuesta transgrede los principios de eficiencia y eficacia previstos en los artículos 3° y 5° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

La entidad en su respuesta acoge lo objetado respecto al retraso en la implementación de la firma electrónica y detalla las actividades realizadas durante los años 2016 y 2017; no obstante, no se pronuncia sobre el pago del primer grupo de firmas, situación que era la observada, motivo por el cual procede mantener lo advertido primitivamente.

CONCLUSIONES

Atendidas las consideraciones expuestas durante el desarrollo del presente trabajo, el Servicio Nacional de la Discapacidad ha aportado antecedentes e iniciado acciones que han permitido salvar parte de las objeciones formuladas en el Preinforme de Observaciones N° 401, de 2017, de esta Contraloría General.

En efecto, la observación planteada en el capítulo I, Aspectos de Control Interno, numeral 3, Falta de código de Ética Formalizado, se levanta, conforme a los nuevos antecedentes aportados por el servicio.

Sin perjuicio de lo indicado, en lo que concierne a los restantes hechos observados, se deberán adoptar medidas con el objeto de dar estricto cumplimiento a las normas legales y reglamentarias que las rigen, entre las cuales se estima necesario considerar, a lo menos, las siguientes:

1. Respecto a lo indicado en el capítulo II, Examen de la Materia Auditada, numeral 1, Sistema de Remuneraciones Global 3000, puntos 1.1, Fraccionamiento de la compra del Sistema de Remuneraciones (C)[6], y 1.2, Ausencia de un acuerdo complementario con la finalidad de resguardar la adquisición de productos y servicios del Convenio Marco ID N° 2239-7-LP14 (C)[7], la repartición deberá instruir un sumario administrativo que establezca las eventuales responsabilidades administrativas de los involucrados en no cautelar los intereses del estado, al permitir la fragmentación de la compra y no caucionar el fiel cumplimiento de los acuerdos suscritos, debiendo remitir a la Unidad de Seguimiento de Fiscalía, copia del acto administrativo que lo ordena en el plazo de 15 días hábiles, contados desde la recepción del presente documento.

2. En lo tocante al capítulo III, Examen de Cuentas, Contratación de los servicios de Firma Electrónica Avanzada, sin utilización (C)[8], el SENADIS deberá incorporar esta materia en el sumario mencionado, con el fin de determinar y hacer efectivas las eventuales responsabilidades administrativas, respecto al monto gastado en certificados de firma electrónica avanzada, los que en definitiva no fueron utilizados, lo que originó una nueva compra de los mismos.

3. Acerca de lo manifestado en el capítulo I, Aspectos de Control Interno, numeral 2, Ausencia en el control de implementación del sistema de remuneraciones (MC)[9], el servicio deberá implementar un formato parametrizado de salida para todos los informes emanados del sistema y desarrollar e implementar el algoritmo que permita calcular automáticamente la Asignación de Modernización, lo que le corresponderá acreditar en el término de 60 días hábiles, contado desde la recepción del presente documento.

4. Respecto a lo indicado en el capítulo II, Examen de la Materia Auditada, numeral 1, Sistema de Remuneraciones Global 3000, punto 1.1, Fraccionamiento de la compra del Sistema de Remuneraciones, la institución, deberá evitar a futuro la reiteración de los hechos descritos y arbitrar las medidas para que, en lo sucesivo, no existan fragmentación de compras.

Para lo indicado en el punto 1.2, Ausencia de un acuerdo complementario con la finalidad de resguardar la adquisición de productos y servicios del Convenio Marco ID N°. 2239-7-LP14, la repartición

---

6 C: Observación compleja, Ausencia de supervisión (valorar, revisar y aprobar, dirigir y capacitar).
7 C: Observación compleja, Ausencia de supervisión (valorar, revisar y aprobar, dirigir y capacitar).
8 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
9 MC: Observación medianamente compleja, Inexistencia de procedimientos formalizado.

deberá, en lo sucesivo, incorporar acuerdos complementarios en aquellos servicios que sean adquiridos mediante la modalidad de convenio marco, con la finalidad de cautelar los intereses del Estado.

En cuanto a lo advertido en el punto 1.3, Falta de una bitácora de actividades de modificación al sistema de remuneración (C)[10], la repartición fiscalizada deberá desarrollar el procedimiento que establezca la obligación de mantener un registro de las actividades realizadas por los usuarios, junto con disponer de la bitácora de actividades reconstruida. Asimismo, respecto de lo objetado sobre las modificaciones a la base de datos por personal externo, corresponde que la entidad habilite y monitoree el log de transacciones de la base de datos del sistema auditado.

En lo referido al punto 1.4, Inexistencia de un funcionario a cargo de las bases de datos(C)[11], el servicio deberá disponer de uno que administre las bases de datos y mantenga la integridad de las mismas.

Sobre lo señalado en el punto 1.5, Sistema de remuneraciones sin segregación de perfiles de usuarios (C)[12], la institución auditada deberá crear los perfiles de usuarios del sistema de remuneraciones, con la correspondiente segregación de funciones en las personas que intervienen el citado aplicativo, remitiendo los perfiles de los usuarios creados, en el término de 60 días hábiles, contado desde la recepción del presente informe final.

En cuanto a lo objetado en el punto 1.6, Inexistencia de un proceso de validación de claves de acceso (C)[13], la repartición deberá remitir el estado de avance de la política de control de acceso, junto con el respaldo de la implementación del a misma, en el período de 60 días desde la recepción del presente informe.

5. Acerca de lo manifestado en el capítulo II, Examen de la materia Auditada, numeral 2, sobre Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos, punto 2.1, Plan de contingencia desactualizado y sin formalizar (C)[14], la repartición deberá remitir el plan de contingencia actualizado y formalizado, junto con el respaldo de su sociabilización, en el término de 60 días hábiles a contar de la recepción del presente informe.

---

10 C: Observación compleja, Falencias de seguridad de sistemas.
11 C: Observación compleja, Falencias de seguridad de sistemas.
12 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
13 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
14 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

En relación a lo indicado en el punto 2.2, Inexistencia de un plan de recuperación ante desastres (C)[15], el SENADIS deberá remitir el plan de recuperación de desastres formalizado, el cual deberá, al menos, considerar los procedimientos necesarios para poder reestablecer los servicios una vez ocurrido el desastre, dentro del plazo de 60 días hábiles desde la recepción de este informe.

En lo que toca al punto 2.3, Ausencia de pruebas al procedimiento de gestión de la continuidad del negocio (C)[16], la institución deberá efectuar pruebas al procedimiento de continuidad del negocio, las que deberán ser documentadas, indicando las acciones realizadas, además de firmadas por los participantes en las actividades que le competen, remitiendo los aludidos antecedentes a esta Entidad de Control en el período de los 60 días hábiles, desde la recepción de este informe final.

Acerca de lo indicado en el punto 2.4, Inexistencia de un LOG de la red (C)[17], el servicio deberá crear y conservar un LOG de las actividades anómalas que ocurran en la red, para lo que dispone de 60 días desde la recepción del presente informe.

Respecto a lo advertido en el punto 2.5, Ausencia de un procedimiento de revisión de permisos de acceso (C)[18], la entidad fiscalizada deberá crear un procedimiento formal que contenga la revisión de los permisos de acceso, indicando la periodicidad, quien lo ejecutará y quien lo revisará. Para lo que dispone de 60 días hábiles contados desde la recepción de este informe final.

En cuanto a lo señalado en el punto 2.6, Intentos fallidos de acceso sin registro (C)[19], el servicio deberá implementar un registro de los intentos fallidos de acceso, que considere a lo menos, los datos ingresados, la fecha y hora en que ocurrió, en el plazo de 60 días hábiles, desde la recepción del presente informe.

---

15 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
16 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
17 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
18 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
19 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

En relación a lo advertido en el punto 2.7, Falta de procedimientos de restauración de respaldo (C)[20], el SENADIS deberá crear un procedimiento de restauración de respaldos que a lo menos contemple el contenido a respaldar, periodicidad con que se efectuará y la persona responsable, en el término de 60 días hábiles desde la recepción del presente informe.

Sobre lo objetado en el punto 2.8, Carencia de un registro de errores y las soluciones ejecutadas (C)[21], la institución auditada deberá crear un registro de los errores que ocurran en los sistemas y documentar las soluciones efectuadas contemplando a lo menos las fechas de ambas situaciones, las personas involucradas en la detección y solución de las mismas.

En lo que atañe al punto 2.9, Ausencia de un registro de cambios en los sistemas de la repartición auditada (C)[22], el servicio deberá crear un registro de cambios a los sistemas, que debe incorporar, a lo menos, la información de los cambios, interacción con otros sistemas, encargado de realizar el cambio y de quien efectuó las pruebas, además de las fechas de cada una de las situaciones, para lo que dispone de 60 días hábiles desde la recepción del presente informe.

Sobre lo indicado en el punto 2.10, Inexistencia de un procedimiento para informar incidentes tecnológicos (C)[23], el SENADIS deberá elaborar un procedimiento que informe los incidentes tecnológicos, el que debe estar debidamente formalizado y conocido por el personal, el cual deberá ser remitido a esta Entidad de Control, en el término de 60 días hábiles desde la recepción del presente informe.

En relación con lo establecido en el punto 2.11, Falta de acciones de seguimiento de los casos de incidentes de seguridad (C)[24], la repartición deberá documentar e implementar el nuevo procedimiento de control y registro de incidentes, incorporando las tereas y responsables del seguimiento, suministrando dicho antecedente en el plazo de 60 días hábiles desde la recepción de este informe final.

---

20 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

21 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

22 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

23 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

24 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

Respecto a lo indicado en el punto 2.12, Carencia de una bitácora de evaluación del sitio web del SENADIS (C)[25], la institución fiscalizada deberá crear una bitácora de evaluación del sitio web, la que debe contemplar a lo menos las actividades efectuadas, informado su estado de avance dentro de 60 días hábiles desde la recepción del presente informe.

Acerca de lo objetado en el punto 2.13, Ausencia de respaldos fuera de las instalaciones (C)[26], el servicio deberá elaborar un estudio de manera que le permita disponer de un lugar alternativo para almacenar los correspondientes respaldos de la información, que considere las características de seguridad e idoneidad similares al site principal, suministrando el mismo en el plazo ya señalado.

En cuanto a lo observado en el punto 2.14, Inexistencia de trazabilidad de acciones efectuadas por usuarios de la base de datos y mecanismos de auditoría (C)[27], la entidad deberá implementar el LOG de la base de datos de manera que permita, al menos, conocer las actividades que registren los datos almacenados y el usuario que lo realizó, de manera que no sea genérico y permita contar con una trazabilidad de la información, comunicando su estado de avance en el plazo indicado precedentemente.

6. Sobre lo advertido en el capítulo II, Examen de la materia Auditada, numeral 3, Falta de un procedimiento para filtrar SPAM (C)[28], el SENADIS deberá crear un procedimiento que permita mitigar y filtrar los SPAM, el que deberá estar formalizado y sociabilizado con el personal, remitiendo el aludido documento dentro de 60 días hábiles desde recepción del presente informe.

7. En relación a lo señalado en igual capítulo, numeral 4, Inexistencia de un documento formalizado para gestionar la seguridad de la información (C)[29], la repartición auditada deberá elaborar un documento que establezca lineamientos para administrar la seguridad de la información, que se encuentre formalizado y sociabilizado en el personal, remitiendo el procedimiento dentro de 60 días hábiles desde recepción del presente informe final.

---

25 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
26 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
27 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
28 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
29 C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

8. En lo tocante al capítulo III, Examen de Cuentas, Contratación de los servicios de Firma Electrónica Avanzada, sin utilización, el SENADIS deberá en lo sucesivo, establecer procedimientos y mejorar sus controles, de modo de evitar que productos y/o servicios no sean utilizados y éstos dejen de ser válidos.

Finalmente, para aquellas observaciones que se mantienen, se deberá remitir el "Informe de Estado de Observaciones" de acuerdo al formato adjunto en Anexo N° 3, en un plazo máximo de 60 días hábiles, contado desde la recepción del presente informe, comunicando las medidas adoptadas y acompañando los antecedentes de respaldo respectivos.

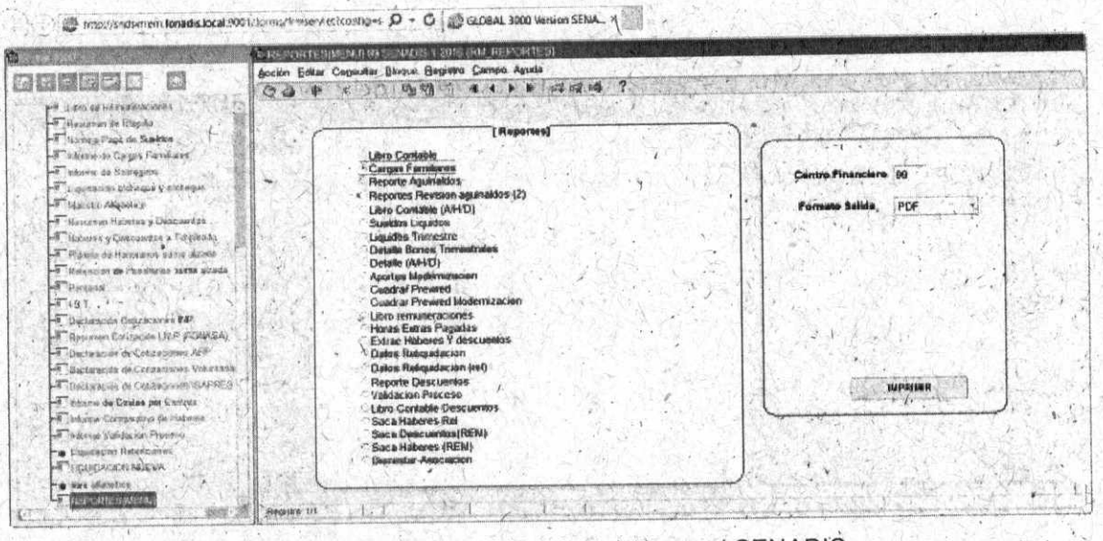
Transcríbase el presente informe al señor Ministro de Desarrollo Social, y a la Auditora del precitado ministerio, al Director Nacional, y a la señora Jefa del Departamento de Auditoría Interna, estos dos últimos del SENADIS.

Saluda atentamente a Ud.,

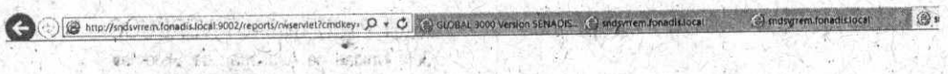
JEAN PAUL THIBAUT VERDUGO
Jefe Unidad de Auditorías de Sistemas
Departamento Auditorías Especiales
Contraloría General de la República

ANEXO N°1

Solicitud de informe de cargas familiares, si bien entrega el dato el formato es el inicial del sistema sin parametrizar ejemplo: "YOUR Inc. COMPANY"



Fuente: Sistema de Remuneraciones Global 3000, instalado en el SENADIS.



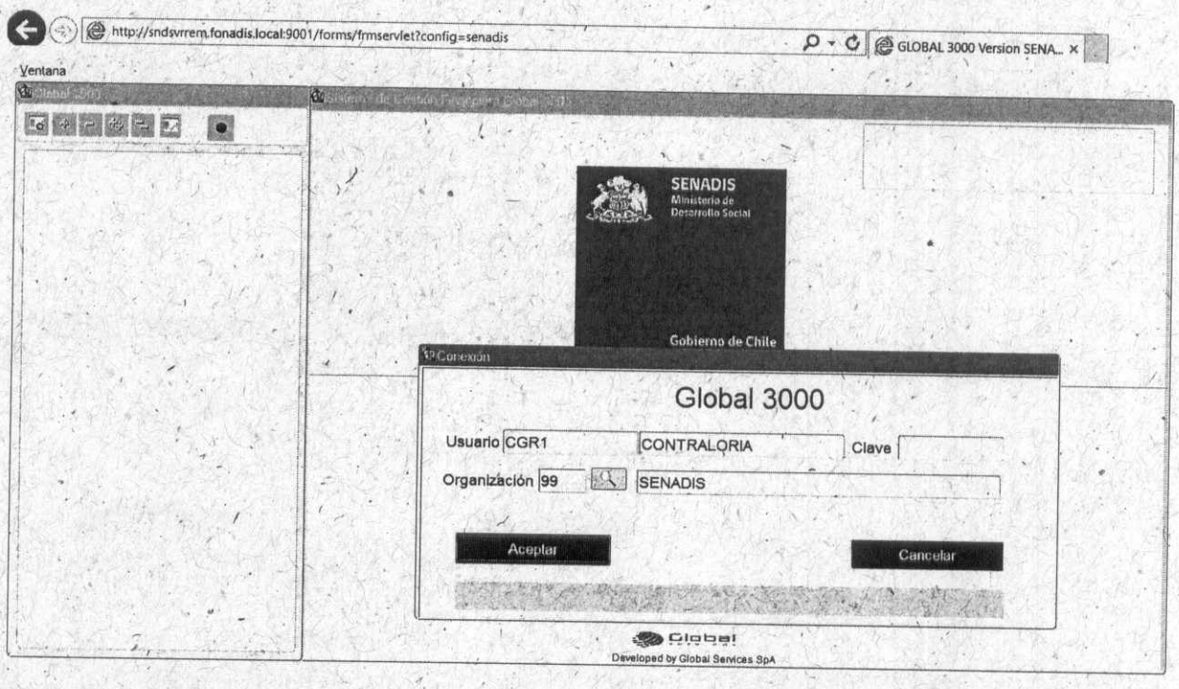
YOUR Inc. COMPANY

Rol Emp						Total Hd
06183149	161502	98477	8441	20647	14068	13026
08589830	201407	122809	10527	33376	17544	16245
09898052	136206	83052	7119	13514	11865	11865
10735304	101271	68098	5837	7016	9728	0
11191410	200706	122809	10527	33432	17544	16245
11403515	170717	106035	9089	24269	0	0
12051411	139656	84713	7261	14253	0	11865
12670252	128879	78176	6701	11233	11168	10949
12693501	160939	98477	8441	20669	14068	13026
13141941	88508	54974	4712	597	7853	7551
13333741	90210	56031	4803	1087	8004	7551
13336509	90902	56461	4839	1286	8066	7908
13527277	193948	118261	10137	29795	16894	16245
13669351	186738	115987	9942	28882	0	16245
13709434	197723	122809	10527	33671	17544	0
13896586	136206	83052	7119	12914	11865	0

Fuente: Sistema de Remuneraciones Global 3000, instalado en el SENADIS.

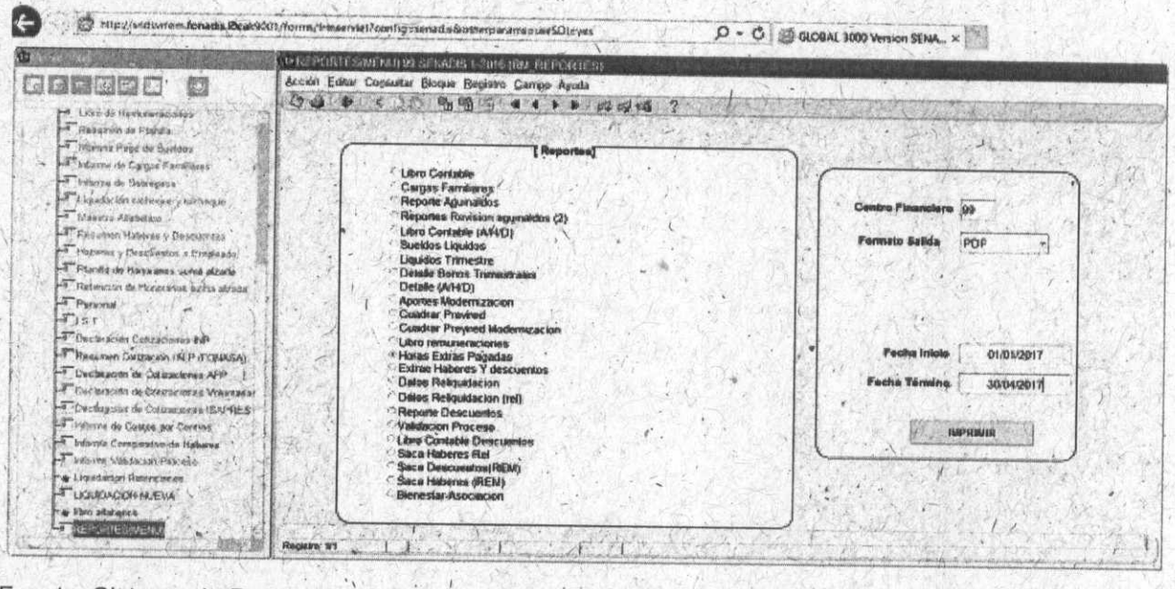
ANEXO N° 2

Pantalla de inicio e ingreso de usuario y clave.



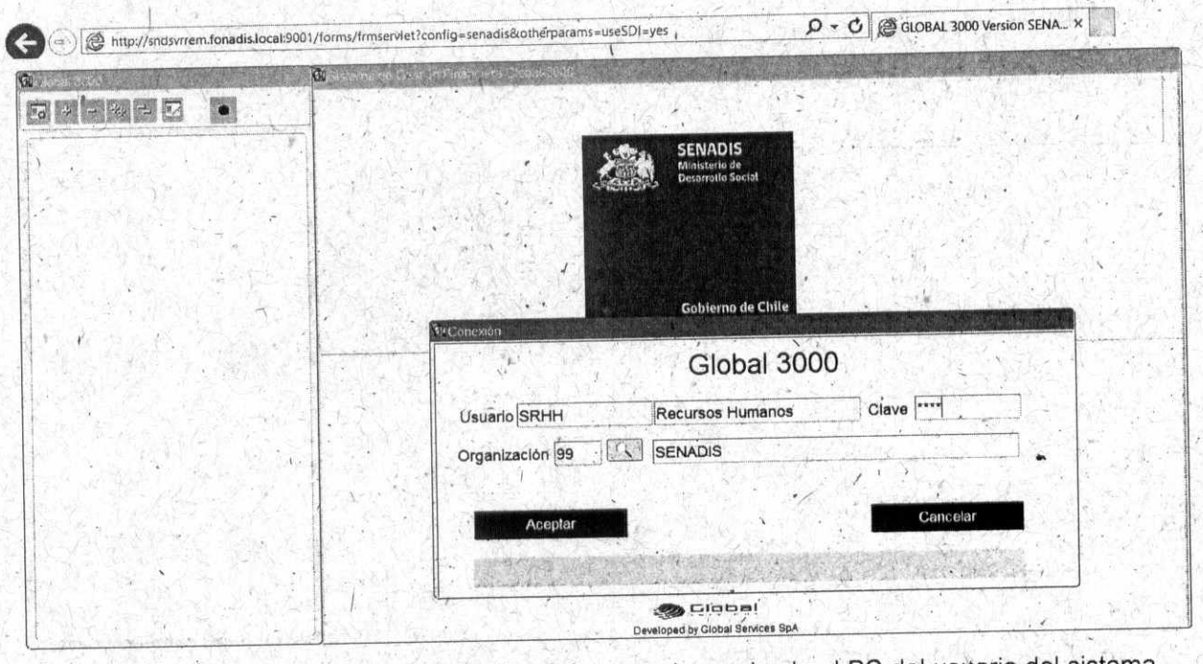
Fuente: Sistema de Remuneraciones Global 3000, instalado en el SENADIS.

Acceso al sistema sin necesidad de ingresar clave.



Fuente: Sistema de Remuneraciones Global 3000, instalado en el SENADIS.

Situación que ocurre con el ingreso como el único usuario del sistema de remuneraciones que está activo en el SENADIS.



Fuente: Captura de pantalla del Sistema de Remuneraciones desde el PC del usuario del sistema de remuneraciones.

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

ANEXO N° 3

Estado de Observaciones del Informe Final N° 401, de 2017.

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo I, Aspectos de Control Interno, numeral 2.	Ausencia en el control de implementación del sistema de remuneraciones.	MC: Observación medianamente compleja, Inexistencia de procedimientos formalizado.	El servicio deberá implementar un formato parametrizado de salida para todos los informes emanados del sistema y desarrollar e implementar el algoritmo que permita calcular automáticamente la Asignación de Modernización, lo que le corresponderá acreditar en el término de 60 días hábiles, contado desde la recepción del presente documento.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 1. Sistema de Remuneraciones Global 3000; punto 1.1.	Fraccionamiento de la compra del Sistema de Remuneraciones.	C: Observación compleja, Ausencia de supervisión (valorar, revisar y aprobar, dirigir y capacitar).	La institución deberá efectuar una investigación sumaria que establezca las eventuales responsabilidades administrativas de los involucrados en no cautelar los intereses del estado permitiendo la fragmentación en la compra y no caucionar el fiel cumplimiento de los acuerdos suscritos, debiendo remitir a la Unidad de Seguimiento de Fiscalía, copia del acto administrativo que lo ordena en el plazo de 15 días hábiles, contado desde la recepción del presente documento.			
Capítulo II. Examen de la Materia Auditada; numeral 1. Sistema de Remuneraciones Global 3000; punto 1.2.	Ausencia de un acuerdo complementario que prevea cauciones.	C: Observación compleja, Ausencia de supervisión (valorar, revisar y aprobar, dirigir y capacitar).				

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 1. Sistema de Remuneraciones Global 3000; punto 1.5.	Sistema de remuneraciones sin segregación de funciones.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La entidad auditada deberá crear los perfiles de usuarios del sistema de remuneraciones, con la correspondiente segregación de funciones de las personas que intervienen el citado aplicativo, remitiendo los perfiles de los usuarios creados, en el término de 60 días hábiles, contados desde la recepción del presente informe final.			
Capítulo II. Examen de la Materia Auditada; numeral 1. Sistema de Remuneraciones Global 3000; punto 1.6.	Inexistencia de validación de claves de acceso.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La repartición deberá remitir el estado de avance de la política de control de acceso, junto con el respaldo de la implementación de la misma, en el período de 60 días hábiles desde la recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.1.	Plan de Contingencia desactualizado y sin formalizar.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La institución deberá remitir el plan de contingencia actualizado y formalizado, junto con el respaldo de su sociabilización, al término de 60 días hábiles a contar de la recepción del presente informe.			
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.2.	Inexistencia de plan de recuperación ante desastres.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	El SENADIS deberá remitir el plan de recuperación de desastres formalizado, el cual deberá al menos considerar los procedimientos necesarios para poder reestablecer los servicios una vez ocurrido el desastre, dentro del plazo de 60 días hábiles, contado desde la recepción de este informe.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.3.	Ausencia de pruebas al procedimiento de gestión de continuidad del negocio.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La repartición deberá efectuar pruebas al procedimiento de continuidad del negocio, las que deberán ser documentadas, indicando las acciones realizadas, además de firmadas por los participantes en las actividades que le competen, remitiendo los aludidos antecedentes a esta Entidad de Control en el período de los 60 días hábiles, desde la recepción de este informe final.			
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.4.	Inexistencia de un LOG de la red.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	El SENADIS deberá crear y conservar un LOG de las actividades anómalas que ocurran en la red, para lo que dispone de 60 días hábiles desde la recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.5.	Ausencia de un procedimiento de revisión de permisos de acceso.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La institución deberá crear un procedimiento formal que contenga la revisión de los permisos de acceso, indicando la periodicidad, quien lo ejecutará y quien lo revisará. Para lo que dispone de 60 días hábiles contados desde la recepción de este informe final.			
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.6.	Intentos fallidos de acceso sin registro.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La entidad fiscalizada tendrá que implementar un registro de los intentos fallidos de acceso que considere, a lo menos, los datos ingresados, la fecha y hora en que ocurrió, en el plazo de 60 días hábiles, desde la recepción del presente informe.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.7.	Falta de procedimientos de restauración de respaldos.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	El SENADIS deberá crear un procedimiento de restauración de respaldos que a lo menos contemple el contenido a respaldar, periodicidad con que se efectuará y la persona responsable, en el término de 60 días hábiles desde la recepción del presente informe.			
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.9.	Ausencia de un registro de cambios en los sistemas.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	El servicio deberá crear un registro de cambios a los sistemas, que incorpore, a lo menos, la información relativa a la interacción con otros sistemas, del encargado de efectuar los cambios y de hacer las pruebas, además de las fechas de cada una de las situaciones, para lo que dispone de 60 días hábiles desde la recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.10.	Inexistencia de un procedimiento para informar incidentes tecnológicos.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	El SENADIS deberá elaborar un procedimiento que informe los incidentes tecnológicos, el que debe estar debidamente formalizado y conocido por el personal, el cual deberá ser remitido a esta Entidad de Control, en el término de 60 días hábiles desde la recepción del presente informe.			
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.11.	Falta de acciones de seguimiento de los incidentes de seguridad.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La institución deberá documentar e implementar el nuevo procedimiento de control y registro de incidentes, incorporando las tereas y responsables del seguimiento, suministrando dicho antecedente en el plazo de 60 días hábiles desde la recepción de este informe final.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.12.	Carencia de bitácora de evaluación de sitio web del SENADIS.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La repartición deberá crear una bitácora de evaluación del sitio web, la que debe contemplar, a lo menos, las actividades efectuadas, informado su estado de avance dentro de 60 días hábiles desde la recepción del presente informe.			
Capítulo II. Examen de la Materia Auditada; numeral 2. Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.13.	Ausencia de respaldo fuera de las instalaciones.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La institución auditada tendrá que elaborar un estudio de manera que le permita disponer de un lugar alternativo para almacenar los respaldos de la información, que considere las características de seguridad e idoneidad similares al site principal, suministrando el mismo en el término de 60 días hábiles desde la recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 2, Incumplimiento de aspectos de seguridad y confidencialidad de los documentos electrónicos; punto 2.14.	Inexistencia de trazabilidad de acciones efectuadas por los usuarios de la base de datos y mecanismos de auditoría.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	El servicio deberá implementar el LOG de la base de datos de manera que permita, al menos, conocer las actividades que registren los datos almacenados y el usuario que lo efectuó, de manera que no sea genérico y permita realizar la trazabilidad de la información, comunicando su estado de avance en el término de 60 días hábiles desde la recepción del presente informe.			
Capítulo II. Examen de la Materia Auditada; numeral 3.	Falta de Procedimiento para filtrar SPAM.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	El SENADIS deberá crear un procedimiento que permita mitigar y filtrar los SPAM, el que deberá estar formalizado y sociabilizado con el personal, remitiendo el aludido documento dentro de 60 días hábiles desde recepción del presente informe.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II. Examen de la Materia Auditada; numeral 4.	Inexistencia de un documento formalizado para gestionar la seguridad de la información.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La repartición auditada deberá elaborar un documento para la gestión de seguridad de la Información que se encuentre formalizado y sociabilizado en el personal, remitiendo el procedimiento antes señalado dentro de 60 días hábiles desde recepción del presente informe final.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
III. Examen de Cuenta.	Contratación de los servicios de Firma electrónica avanzada, sin utilización.	C: Observación compleja, Incumplimiento de la normativa contenida en los decretos Nos 77, 81 y 83, los 3 del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	El Servicio Nacional de la Discapacidad deberá instruir una investigación sumaria, con el fin de determinar y hacer efectivas las eventuales responsabilidades administrativas, respecto al monto gastado en certificados de firma electrónica avanzada, los que en definitiva no fueron utilizados, debiendo remitir a la Unidad de Seguimiento de Fiscalía de esta Contraloría General, el acto administrativo que disponga tal proceso disciplinario y designe fiscal, en el término de 15 días hábiles contado desde la recepción del presente informe. Además, deberá remitir la documentación sustentante que dé cuenta del uso del segundo paquete de firmas, individualizado.			